JOURNAL OF NUMBER THEORY **61**, 283–291 (1996)
ARTICLE NO. 0149

Automorphism Polynomials in Cyclic Cubic Extensions

Robin J. Chapman*

Department of Mathematics, University of Exeter, Exeter EX4 4QE, United Kingdom

Communicated by D. J. Lewis

Received June 1, 1995; revised April 15, 1996

We provide simple proofs of the main results in the paper by Patrick Morton, "Characterizing Cyclic Cubic Extensions by Automorphism Polynomials" (*J. Number Theory* **49** (1994), 183–208), avoiding the use of computer algebra.

1. INTRODUCTION

In [2] Morton considers cyclic cubic extensions F/κ of fields. If σ is a generator of the Galois group of this extension, he shows that if $\theta \in F$ and $\sigma(\theta) = \theta^2 + u$ $(u \in \kappa)$ then, provided $\operatorname{char} \kappa \neq 2$, $u = -(1/4)(s^2 + 7)$ where $s \in \kappa$ and the field F is determined by s. He also proves a theorem showing when two values of the parameter $s \in \kappa$ give the same extension field and develops an analogue of Kummer theory, not assuming that κ contains the third roots of unity, describing the exponent 3 Abelian extensions of κ. However, some of his proofs rely on extensive Mathematica computation, and he asks if there are less computationally demanding proofs.

In this paper I relate Morton's analogue of Kummer theory to classical Kummer theory and Artin–Schreier theory. In this way I provide much simpler proofs of Morton's results.

2. THE GENERIC CASE

We first deal with the case where $\operatorname{char} \kappa \neq 3$ and κ does not have a primitive cube root of unity. In this case let $\kappa' = \kappa(\zeta)$ where ζ is a primitive cube root of unity. The extension κ'/κ is quadratic; let τ be its non-trivial automorphism. If $\lambda \in \kappa'$ for convenience we shall write $\overline{\lambda} = \tau(\lambda)$, $N(\lambda) = \lambda\overline{\lambda}$, and $T(\lambda) = \lambda + \overline{\lambda}$.

If F/κ is a cyclic cubic extension, then $F' = F(\zeta)$ is a cyclic cubic extension of κ' and a cyclic sextic extension of κ. Conversely each cyclic sextic

* E-mail: rjc@maths.exeter.ac.uk.

0022-314X/96 $18.00

extension of κ which contains κ' contains a unique cyclic cubic extension of κ. By using the Kummer theory of κ' we can identify all such extensions.

PROPOSITION 1. *Let κ be a field not of characteristic* 3 *and not containing a primitive cube root of unity, and let $\kappa' = \kappa(\zeta)$ where ζ is a primitive cube root of unity. Then a field $F' \supseteq \kappa'$ is a cyclic sextic extension of κ if and only if $F' = \kappa'(\beta)$ with $\beta^3 = \delta^2\bar{\delta}$ where $\delta \in \kappa'$ and $\delta^2\bar{\delta}$ is not a cube in κ'.*

Proof. Suppose that $F' \supseteq \kappa'$ is a cyclic sextic extension of κ. Let σ and τ be automorphisms of F'/κ of degrees 3 and 2 respectively. Note that τ restricts to the automorphism of κ'/κ that we have already labelled τ. By Kummer theory (see, e.g., Lang [1, Chap. VIII, Sect. 8]) $F' = \kappa'(\beta)$ where $\beta^3 = \alpha \in \kappa'^*$, α is not a cube in κ', and $\sigma(\beta) = \zeta\beta$. As the automorphisms σ and τ commute then

$$\sigma(\tau(\beta)) = \tau(\sigma(\beta)) = \tau(\zeta\beta) = \zeta^{-1}\tau(\beta).$$

If $r = \beta\tau(\beta)$ then trivially $\tau(r) = r$ and also

$$\sigma(r) = \sigma(\beta)\,\sigma(\tau(\beta)) = \beta\tau(\beta) = r.$$

Hence $r \in \kappa$. Also,

$$r^3 = \beta^3\tau(\beta^3) = \alpha\bar{\alpha} = N(\alpha).$$

If we put $\delta = \alpha/r$ then

$$N(\delta) = N(\alpha)/r^2 = r$$

and

$$\delta^2\bar{\delta} = \alpha^2\bar{\alpha}/r^3 = \alpha = \beta^3,$$

and so F' is of the claimed form.

Conversely suppose that $\delta \in \kappa'$ and $\delta^2\bar{\delta}$ is not a cube in κ'. Then $F' = \kappa'(\beta)$ where $\beta^3 = \delta^2\bar{\delta}$ is a cyclic cubic extension of κ' whose Galois group is generated by σ with $\sigma(\beta) = \zeta\beta$. If $\beta' = N(\delta)/\beta$ then $\beta'^3 = \delta\bar{\delta}^2 = \tau(\delta^2\bar{\delta})$. It is clear that we can extend the automorphism τ of κ'/κ to a κ-automorphism of F' via $\tau(\beta) = \beta'$. As $\tau(\beta') = \bar{\delta}\delta/\beta' = \beta$ then τ has order 2. Also,

$$\tau(\sigma(\beta)) = \tau(\zeta\beta) = \zeta^{-1}\beta' = N(\delta)/(\zeta\beta) = \sigma(N(\delta)/\beta) = \sigma(\tau(\beta))$$

and so σ and τ commute. As σ has order 3, then the extension F'/κ is cyclic sextic. The proof is now complete. ∎

For $\delta \in \kappa'$ let $F'_\delta = \kappa'(\beta)$ with $\beta^3 = \delta^2\bar{\delta}$. If $\delta^2\bar{\delta}$ is not a cube in κ' then F'_δ/κ contains a cubic subextension F_δ/κ. We now seek to identify this extension.

PROPOSITION 2. *Let $\delta \in \kappa'$ with $\delta^2\bar{\delta}$ not a cube in κ'. Then $F_\delta = \kappa(\psi)$ where ψ has minimal polynomial*

$$X^3 - 3N(\delta)\, X - N(\delta)\, T(\delta).$$

over κ.

Proof. Note that F_δ is the fixed field of τ acting on F'_δ. If $\psi = \beta + \tau(\beta) = \beta + N(\delta)/\beta$ then certainly $\psi \in F'_\delta$.

As β and $\tau(\beta)$ are the roots of $x^2 - \psi x + N(\delta) = 0$, then F'_δ is quadratic over $\kappa(\psi)$ and so $F_\delta = \kappa(\psi)$. Now

$$\psi^3 = \beta^3 + \tau(\beta)^3 + 3\beta\tau(\beta)(\beta + \tau(\beta)) = \delta^2\bar{\delta} + \delta\bar{\delta}^2 + 3\delta\bar{\delta}\psi$$

and so the minimal polynomial of ψ over κ is

$$X^3 - 3N(\delta)\, X - N(\delta)\, T(\delta). \quad \blacksquare$$

To relate this element ψ to the element θ constructed by Morton, we need to work out the action of the automorphisms of F_δ/k on ψ.

PROPOSITION 3. *Let $\delta = a + b\bar{\zeta} \in \kappa'$ with $\delta^2\bar{\delta}$ not a cube in κ'. If σ is the automorphism of F'_δ/κ' taking β to $\zeta\beta$ then*

$$\sigma(\psi) = \frac{1}{b}(\psi^2 - a\psi - 2N(\delta))$$

and

$$\sigma^2(\psi) = \frac{1}{b}(-\psi^2 + (a-b)\,\psi + 2N(\delta)).$$

Proof. We calculate

$$\begin{aligned}
\psi^2 &= \beta^2 + \tau(\beta)^2 + 2\beta\tau(\beta) \\
&= \delta^2\bar{\delta}/\beta + \delta\bar{\delta}^2/\tau(\beta) + 2N(\delta) \\
&= \delta\tau(\beta) + \bar{\delta}\beta + 2N(\delta) \\
&= a\psi + b(\bar{\zeta}\tau(\beta) + \zeta\beta) + 2N(\delta).
\end{aligned}$$

But as $\sigma(\psi) = \zeta\beta + \bar{\zeta}\tau(\beta)$ then

$$\sigma(\psi) = \frac{1}{b}(\psi^2 - a\psi - 2N(\delta)).$$

As the X^2-term in the minimal polynomial of ψ vanishes, it is immediate that

$$\sigma^2(\psi) = -\psi - \sigma(\psi) = \frac{1}{b}(-\psi^2 + (a-b)\,\psi + 2N(\delta)). \quad \blacksquare$$

Suppose also that $\operatorname{char}\kappa \neq 2$. If we put $\theta = \psi/b - a/2b$ then a straightforward computation gives

$$\sigma(\theta) = \theta^2 - \frac{8N(\delta) + a^2 + 2ab}{4b^2} = \theta^2 - \frac{9a^2 - 6ab + 8b^2}{4b^2}$$

and that

$$\theta^3 + \frac{3a}{2b}\theta^2 + \frac{3(a^2 - 4N(\delta))}{4b^2}\theta + \frac{a^3 - 12aN(\delta) - N(\delta)\,T(\delta)}{8b^3} = 0.$$

If we choose $\delta = s + 2 + 3\zeta = s - 1 - 3\bar{\zeta}$ we get

$$\sigma(\theta) = \theta^2 - \tfrac{1}{4}(s^2 + 7)$$

and

$$\theta^3 + \tfrac{1}{2}(1-s)\,\theta^2 - \tfrac{1}{4}(s^2 + 2s + 9)\,\theta + \tfrac{1}{8}(s^3 + s^2 + 7s - 1) = 0.$$

This shows that $\theta + \sigma(\theta) + \sigma^2(\theta) = (1/2)(s-1)$ and so

$$\sigma^2(\theta) = -\theta^2 - \theta + \tfrac{1}{4}(s^2 + 2s + 5),$$

giving the equations (2) and (3) of [2].

We now turn to the question of when two values of δ give the same field.

PROPOSITION 4. *If $\delta \in \kappa'^*$ then $\delta^2\bar{\delta}$ is a cube in κ' if and only if $\delta \in \kappa^*(\kappa'^*)^3$. Let $\delta_1, \delta_2 \in \kappa'^*$. The fields F_{δ_1} and F_{δ_2} are equal if and only if $\delta_1/\delta_2 \in \kappa^*(\kappa'^*)^3$ or $\delta_1/\bar{\delta}_2 \in \kappa^*(\kappa'^*)^3$.* $\blacksquare$

Proof. If $\delta = r\gamma^3$ with $r \in \kappa$ and $\gamma \in \kappa'$, then $\delta^2\bar{\delta} = (r\gamma^2\bar{\gamma})^3$. Conversely, if $\delta^2\bar{\delta} = \eta^3$ with $\eta \in \kappa'$ then $\delta = N(\delta)^{-1}\,\eta^3 \in \kappa^*(\kappa'^*)^3$.

Now $F_{\delta_1} = F_{\delta_2}$ if and only if $F'_{\delta_1} = F'_{\delta_2}$. By Kummer theory this holds if and only if $(\delta_1^2\bar{\delta}_1)/(\delta_2^2\bar{\delta}_2)^{\pm 1} \in (\kappa'^*)^3$. But $(\delta_1^2\bar{\delta}_1)/(\delta_2^2\bar{\delta}_2) = (\delta_1/\delta_2)^2\,\overline{(\delta_1/\delta_2)} \in (\kappa'^*)^3$ if and only if $\delta_1/\delta_2 \in \kappa^*(\kappa'^*)^3$. Similarly, $(\delta_1^2\bar{\delta}_1)(\delta_2^2\bar{\delta}_2) = (\delta_1\delta_2)^2\,\overline{(\delta_1\delta_2)} \in (\kappa'^*)^3$ if and only if $\delta_1\delta_2 \in \kappa^*(\kappa'^*)^3$. As $\delta_2\bar{\delta}_2 \in \kappa$ this happens if and only if $\delta_1/\bar{\delta}_2 \in \kappa^*(\kappa'^*)^3$. ∎

COROLLARY 1. (a) *Suppose that* $\operatorname{char}\kappa \neq 2$. *If* $\delta = s + 2 + 3\zeta$ $(s \in \kappa)$ *then* $\delta^2\bar{\delta} \in \kappa'^3$ *if and only if there exists* $t \in \kappa$ $(t \neq \pm 1)$ *with*

$$s = \frac{t^3 - t^2 - 9t + 1}{2(t^2 - 1)}.$$

In general, even if the characteristic of κ *is* 2, *then* $\delta^2\bar{\delta} \in \kappa'^3$ *if and only if there exists* $p \in \kappa$ $(p \neq 0, \pm 1)$ *with*

$$s = \frac{1 - 2p - p^2 + p^3}{p - p^2}.$$

(b) *Let* $\delta_1 = s + 2 + 3\zeta$ *and* $\delta_2 = v + 2 + 3\zeta$ $(s, v \in \kappa)$. *Then* $F_{\delta_1} = F_{\delta_2}$ *if and only if there exists* $p \in \kappa$ *such that either*

$$v = \frac{s(p^3 - p^2 - 2p + 1) + 7p^2 - 7p}{s(-p^2 + p) + p^3 - 2p^2 - p + 1}$$

or

$$v = -\frac{s(p^3 - 2p^2 - p + 1) + p^3 + 5p^2 - 8p + 1}{s(-p^2 + p) + p^3 - 2p^2 - p + 1}.$$

Proof. (a) By the proposition $\delta^2\bar{\delta}$ is a cube if and only if $\delta = r\eta^3$ with $r \in \kappa$ and $\eta \in \kappa'$. Certainly $\eta \notin \kappa$ and so, absorbing a factor in κ into r, we may assume that $\eta = t + \sqrt{-3}$ (where $\zeta = (1/2)(-1 + \sqrt{-3})$). Hence

$$\eta^3 = t^3 - 9t + (t^2 - 1)\,3\sqrt{-3} = t^3 + 3t^2 - 9t - 3 + 6(t^2 - 1)\,\zeta$$

which is a κ-multiple of $s + 2 + 3\zeta$ if and only if

$$s + 2 = \frac{t^3 + 3t^2 - 9t - 3}{2(t^2 - 1)},$$

i.e.,

$$s = \frac{t^3 - t^2 - 9t + 1}{2(t^2 - 1)}.$$

Alternatively we may suppose that $\eta = 1 + p\zeta$ (if $\eta/\zeta \in \kappa$ then $\eta^3 \in \kappa$ which is false). Then

$$\eta^3 = 1 + 3p\zeta + 3p^2\zeta^2 + p^3 = 1 - 3p^2 + p^3 + 3(p - p^2)\,\zeta$$

which is a κ-multiple of $s + 2 + 3\zeta$ if and only if

$$s + 2 = \frac{1 - 3p^2 + p^3}{p - p^2},$$

i.e.,

$$s = \frac{1 - 2p - p^2 + p^3}{p - p^2}.$$

(b) First suppose that $r \in \kappa$ and $\eta \in \kappa'$ and $\delta_2 = r\eta^3\delta_1$. If η is a κ-multiple of ζ then $\eta^3 \in \kappa$ and we swiftly get $v = s$. Otherwise we may assume that $\eta = 1 + p\zeta$ $(p \in \kappa)$. We calculate

$$\begin{aligned}
\delta_1\eta^3 &= (s + 2 + 3\zeta)(1 + p\zeta)^3 \\
&= (s + 2 + 3\zeta)(1 + p^3 + 3p\zeta + 3p^2\zeta^2) \\
&= [(s + 2)(1 + p^3) + 9p^2] + [3(s + 2)\,p + 3(1 + p^3)]\,\zeta \\
&\quad + [3(s + 2)\,p^2 + 9p]\,\zeta^2 \\
&= [s(p^3 - 3p^2 + 1) + 2p^3 + 3p^2 - 9p + 2] \\
&\quad + 3[s(-p^2 + p) + p^3 - 2p^2 - p + 1]\,\zeta
\end{aligned}$$

which is a κ-multiple of $\delta_2 = v + 2 + 3\zeta$ if and only if

$$v + 2 = \frac{s(p^3 - 3p^2 + 1) + 2p^3 + 3p^2 - 9p + 2}{s(-p^2 + p) + p^3 - 2p^2 - p + 1},$$

i.e.,

$$v = \frac{s(p^3 - p^2 - 2p + 1) + 7p^2 - 7p}{s(-p^2 + p) + p^3 - 2p^2 - p + 1}.$$

Now if $\delta_1/\bar{\delta}_2 \in \kappa^*(\kappa'^*)^3$ then $\delta_2 = r\,\overline{\eta^3\delta_1}$ where $r \in \kappa$ and we may assume that $\eta = 1 + p\zeta$ $(p \in \kappa)$. Repeating the above computation yields $\delta_2 = t\overline{(v' + 2 + 3\zeta)}$ where $t \in \kappa$ and

$$v' = \frac{s(p^3 - p^2 - 2p + 1) + 7p^2 - 7p}{s(-p^2 + p) + p^3 - 2p^2 - p + 1}.$$

But as $(v'+2+3\zeta)=v'-1-3\zeta$ then $t=-1$ and

$$v=-1-v'=-\frac{s(p^3-2p^2-p+1)+p^3+5p^2-8p+1}{s(-p^2+p)+p^3-2p^2-p+1}. \quad \blacksquare$$

We now consider the subfields of the compositum of two cyclic cubic extensions.

PROPOSITION 5. *Let F_{δ_1} and F_{δ_2} be two distinct cyclic cubic extensions of κ where $\delta_1=s+2+3\zeta$ and $\delta_2=t+2+3\zeta$ $(s, t\in\kappa)$. Then the other two cubic subextensions of the compositum $F_{\delta_1}\cdot F_{\delta_2}$ are F_{δ_3} and F_{δ_4} where*

$$\delta_3=\frac{st-7}{s+t+1}+2+3\zeta$$

and

$$\delta_4=\frac{st+t+7}{s-t}+2+3\zeta.$$

Proof. By Kummer theory the cubic subextensions of $(F'_{\delta_1}\cdot F'_{\delta_2})/\kappa'$ are F'_{δ_1}, F'_{δ_2}, $\kappa'(((\delta_1^2\bar{\delta}_1)(\delta_2^2\bar{\delta}_2))^{1/3})=F'_{\delta_1\delta_2}$ and $k'(((\delta_1^2\bar{\delta}_1)^{-1}(\delta_2^2\bar{\delta}_2))^{1/3})=F'_{\bar{\delta}_1\delta_2}$ Hence the cubic extensions κ we seek are $F_{\delta_1\delta_2}$ and $F_{\bar{\delta}_1\delta_2}$.

$$\begin{aligned}\delta_1\delta_2&=(s+2+3\zeta)(t+2+3\zeta)\\&=(s+2)(t+2)+3(s+t+4)\,\zeta+9\zeta^2\\&=(st+2s+2t-5)+3(s+t+1)\,\zeta\\&=(s+t+1)\left(\frac{st-7}{s+t+1}+2+3\zeta\right).\end{aligned}$$

Similarly,

$$\begin{aligned}\bar{\delta}_1\delta_2&=(s+2+3\bar{\zeta})(t+2+3\zeta)\\&=(s+2)(t+2)+9+3(s+2)\,\zeta+3(t+2)\,\bar{\zeta}\\&=(st+2s-t+7)+3(s-t)\,\zeta\\&=(s-t)\left(\frac{st+t+7}{s-t}+2+3\zeta\right). \quad \blacksquare\end{aligned}$$

3. EXCEPTIONAL CASES

We briefly deal here with the two exceptional cases: the first is where κ contains a primitive cube root ζ of unity, and the second is where char $\kappa = 3$. If $\zeta \in \kappa$ then put $\overline{\zeta} = \zeta^2$. If F/κ is a cyclic extension whose Galois group is generated by σ, then the action of σ splits F into three eigenspaces $F_0 = \kappa$, F_1 and F_2, each of κ-dimension one, where

$$F_j = \{x \in F : \sigma(x) = \zeta^j x\}.$$

Note that the trace map from F to κ vanishes on F_1 and F_2. If $\psi = \beta_1 + \beta_2$ is a typical element of $F_1 \oplus F_2$ with $\beta_i \in F_i$, then $\sigma(\beta_1\beta_2) = \beta_1\beta_2$ so that $\beta_1\beta_2 \in \kappa$. Also, $\beta_1^3 = \alpha_1 \in \kappa$ and $\beta_2^3 = \alpha_2 \in \kappa$. If $\beta_1 = 0$ then $\sigma(\psi) = \overline{\zeta}\psi$ and the automorphism polynomials of $u + v\psi$ are linear for all $u, v \in \kappa$. A similar phenomenon happens when $\beta_2 = 0$. Suppose that $\beta_1\beta_2 \neq 0$. Then $\alpha_1 = \delta_1^2\delta_2$ and $\alpha_2 = \delta_1\delta^2$ where $\delta_j = \alpha_j/(\beta_1\beta_2)$. We let κ' be the algebra $\kappa \times \kappa$. Consider κ as a subring of κ' via the embedding $x \mapsto (x, x)$. Then $\kappa' = \kappa[\boldsymbol{\zeta}]$ where $\boldsymbol{\zeta} = (\zeta, \overline{\zeta})$. Now $\psi = \psi(\boldsymbol{\delta})$ is determined by $\boldsymbol{\delta} = (\delta_1, \delta_2) \in \kappa'^*$, and $\delta_1^2\delta_2 \in \kappa^{*3}$ if and only if $\delta_1\delta_2^2 \in \kappa^{*3}$ if and only if $\boldsymbol{\delta} \in \kappa^* \cdot \kappa'^{*3}$. Also, $\kappa(\psi(\boldsymbol{\delta}')) = \kappa(\psi(\boldsymbol{\delta}))$ if and only if $\boldsymbol{\delta}'\boldsymbol{\delta}^{\pm 1} \in \kappa^* \cdot \kappa'^{*3}$. Choosing $\boldsymbol{\delta} = s + 2 + 3\boldsymbol{\zeta}$ gives all non-trivial extensions. Also, if $\boldsymbol{\delta}'\boldsymbol{\delta}^{-1} \in \kappa^* \cdot \kappa'^{*3}$ we can write $\boldsymbol{\delta}' = r(1 + p\boldsymbol{\zeta})^3\,\boldsymbol{\delta}$ with r, $p \in \beta$, but to ensure that $(1 + p\boldsymbol{\zeta}) \neq 0$ we need the extra stipulation that $p \neq -\zeta$ or $-\overline{\zeta}$. We can now obtain the analogues of all the results in the previous section.

Now suppose that κ has characteristic 3. Let F be a cyclic cubic extension of κ, and let σ be a generator of its Galois group. By Artin–Schreier theory $F = \kappa(\alpha)$ where $\sigma(\alpha) = \alpha + 1$ and $\alpha^3 - \alpha = \gamma \in \kappa$. The κ-subspace of trace zero elements of L is generated by 1 and α, and it is easy to see that $\sigma(x)$ is linear in x whenever x lies in this space. Consider $\beta = \alpha^2$, so $\sigma(\beta) = \alpha^2 - \alpha + 1$. But

$$\beta^2 = \alpha^4 = \alpha(\alpha + \gamma) = \beta + \gamma\alpha$$

and so $\alpha = (\beta^2 - \beta)/\gamma$. It follows that

$$\sigma(\beta) = \frac{\beta}{\alpha} + \frac{\alpha - 1}{\alpha}\beta + 1$$

and so if $\theta = (v + 1 - \alpha)/\alpha$ then

$$\sigma(\theta) = \theta^2 + \frac{\alpha^2 + \alpha - 1}{\alpha^2} = \theta^2 - \left[\left(\frac{1 + \alpha}{\alpha}\right)^2 + 1\right].$$

Thus we define $s=(1+\alpha)/\alpha$ so that $\alpha=1/(s-1)$. Note that $\beta+\sigma(\beta)+\sigma^2(\beta)=\alpha^2+(\alpha+1)^2+(\alpha-1)^2=-1$ so that $\theta+\sigma(\theta)+\sigma^2(\theta)=-1/\alpha=1-s$. It follows that

$$\sigma^2(\theta)=-\theta^2-\theta+(s^2-s-1).$$

The condition that L be a non-trivial extension of κ is that $\alpha\neq r^3-r$ for $r\in\kappa$. But $\alpha=r^3-r$ implies that

$$s=\frac{r^3-r+1}{r(r^2-1)}=-\frac{t^3-t^2+1}{t^2-1}$$

if $t=1/r$. Also, two values of the s parameter, s and v, say, give the same field if and only if $1/(v-1)=\pm 1/(s-1)+u^3-u$ where $u\in\kappa$. With the $+$ sign this gives

$$v=\frac{s(u^3-u+1)-(u^3-u)}{s(u^3-u)-(u^3-u-1)}$$

or, setting $u=1/(p+1)$,

$$v=\frac{s(p^3-p^2+p+1)+(p^2-p)}{-s(p^2-p)+(p^3+p^2-p+1)}.$$

Similarly, the $-$ sign gives

$$v=\frac{s(p^3+p^2-p+1)+(p^3-p^2+p+1)}{-s(p^2-p)+(p^3+p^2-p+1)}.$$

If we look at the compositum of the extensions with parameters s and t, the parameters v and w of its other cubic subextensions are given by $1/(v-1)=1/(s-1)+1/(t-1)$ and $1/(w-1)=1/(t-1)-1/(s-1)$, yielding

$$v=\frac{st-1}{s+t+1}\qquad\text{and}\qquad w=\frac{st+t+1}{s-t}.$$

REFERENCES

1. S. Lang, "Algebra," 2nd ed., Addison–Wesley, Menlo Park, CA, 1984.
2. P. Morton, Characterizing cyclic cubic extensions by automorphism polynomials, *J. Number Theory* **49** (1994), 183–208.